

~~TOP SECRET~~
NSA Declassification/Release Instructions on File

TOP SECRET

COMMENTS BY THE DIRECTOR, NATIONAL SECURITY AGENCY

on

CERTAIN RECOMMENDATIONS OF THE HOOVER
COMMISSION (GENERAL MARK CLARK) REPORT

The following comments are offered on the recommendations contained in the inclosure to CSB # 00011:

1. Recommendation No. 4: That the military Services and NSA continue to strive for a higher degree of cryptographic security; that the problem of communications security, including plain text messages and traffic analysis of encrypted messages, be restudied by USCSB (or the Combined Board as recommended in this Report) with a view toward reducing to the lowest practicable level the quantity of information released through telecommunications; and that NSC 168 be re-examined to ascertain if the Director, NSA, has sufficient authority to carry out his COMSEC responsibilities.

Comment: It should be understood that the "problem of communications security" which encompasses the whole field of security of telecommunications has not been studied by USCSB. Members of USCSB are currently furnishing their views to the Chairman, USCSB, on transmission security, one of the components of communications security, including the desirability of a study by USCSB of this problem. I concur completely in the need for this study.

As to better cryptographic security, which is another component of communications security, I have no real doubts as to the high degree of security provided by the cryptoprinciples employed today in U.S. cryptosystems, if properly used, particularly where long-term security is required. Efforts must be continued to reduce the effects of human error in the operation of cryptosystems. Adequate training of operators and retention of trained operators will bring about improvements. Emphasis must continue on simplification of operating procedures both in current cryptosystems and those under development. Greater reliability in equipments must be achieved in order to prevent machine failures which are a contributing factor in some cryptographic compromises. The use of more reliable components is a constant objective in my research and development on communications security equipments.

Recommendation No. 4 points out a very basic fault now existing in national telecommunications, that is, the release of information through telecommunications because of faulty transmission security practices and the considerable amount of intelligence derivable from plain-text, or unclassified messages. In connection with this problem and the recommended review of NSC 168, I recommend strongly the granting of authority to the Director, NSA, to prescribe minimum standards for development of communications procedures which will provide and maintain security of transmissions. A mechanism should be established at that same time to assure compliance by all departments and agencies with these minimum standards.

NSA TS CONTL NO 551561A
COPY NUMBER
PAGE 1 OF 4 PAGES

25X1 TS# 179251-A
Page 1 of 4 pages
Copy 7 of 7 copies

~~TOP SECRET~~

TOP SECRET

TOP SECRET

2. Recommendation No. 5: That a single Board with appropriate technical subcommittees have policy cognizance over communications intelligence and communications security. If the recommendation to place the evaluation and analysis of ELINT under NSA is adopted, then policy guidance for ELINT as well as COMINT and COMSEC should be exercised by the proposed single Board.

Comment: I support this recommendation for a single Board having policy cognizance over COMINT and COMSEC. The issuance of NSCID No. 17 has expanded the authority of USCIB to include policy making for ELINT. Adoption of Recommendation No. 5 need not, therefore, be made contingent upon placing the evaluation and analysis of ELINT under the Director NSA.

3. Before making any specific comments on the following recommendations, I wish to emphasize this point: Communications is a service, not an end in itself. The role of the communicator in the intelligence field must be strictly advisory. Requirements laid on communicators by intelligence people should be well considered and in consonance with the capabilities and limitations of communications, but under no circumstances should communicators be given authority to challenge the validity of the requirements placed on them. Additionally, I want to make it clear that the statements contained in the narrative portion of Part 2 of the Appendix do not in all cases accord with the facts.

4. Recommendation No. 8: That the present basic communications (cryptographic) security plan, providing for centralized control with effective decentralization of operations, be continued; that each agency and service maintain effective inspection and vigorous training programs to reduce to the minimum cryptographic operational security violations.

Comment: I concur in the recommendation but must point out that cryptographic security is but one aspect of over-all communications security. The recent analysis of transmission security by the Chairman, USCSB provides another view of the security of national telecommunications. In this connection, I refer to my comments above on Recommendation No. 4 regarding the need for revising NSC 168.

5. Recommendation No. 9: That NSC determine ways and means to control more effectively release of valuable intelligence to potential enemies via clear text messages being transmitted over government and civil communications networks.

Comment: I indorse the proposal, within limits; presumably, the Task Force would not advocate peacetime censorship of all clear-text communications over government and civil communications networks. I believe that the problem of plain text communications is definitely a factor in over-all transmission security. For this reason, I recommend instead of

NSA TS CONTL NO 551561A
COPY NUMBER
PAGE 2 OF 4 PAGES

TS# 179251-A
Page 2 of 4 pages

TOP SECRET

~~TOP SECRET~~

TOP SECRET

NSC consideration that this should be made a part of a study to be undertaken by USCSB, as contemplated in the comments on Recommendation No. 4, and that recommendations, as appropriate, be submitted to the NSC by USCSB.

The study should consider whether to divorce encryption from classification and whether to require encryption of all electrically transmitted messages. Consideration should be given to the current availability of means for encryption of traffic regardless of classification. An answer to the leakage of information from plain-text messages transmitted over government networks is link encryption. New equipments capable of link encryption are now being developed and should provide an adequate solution to this problem. I have adopted as my COMSEC policy the principle of link encryption for all long line radio communications. I suggest that USCSB, rather than NSC, review this situation as a corollary to its study of transmission security deficiencies.

6. Recommendation No. 10: That the general tendency within the communications intelligence and the communications security agencies to overemphasize the special security facts of their operations with respect to basic communications and electronics features be examined objectively and comprehensively by competent, technically qualified authority to insure that such over emphasis is not producing unnecessary duplication of facilities and operations in peacetime which will grow to completely unrealistic figures in wartime, and producing a system which may fail in an emergency because it will require considerable readjustment of basic operational practices at a critical time. (This service could be accomplished by the subcommittee proposed in Recommendation No. 1 above).

Comment: The flat statement that there exists a "general tendency within the COMINT and COMSEC agencies to overemphasize the special security facets of their operations" is made without supporting evidence. I am sure that the need for special security of COMINT is recognized by those familiar with COMINT matters. In COMSEC certain phases, such as the analysis and evaluation of our own systems, full use is made of COMINT techniques and facilities. These portions of COMSEC must, for this reason, be afforded the same safeguards imposed for protection of COMINT. This aspect of COMSEC is not duplicated outside NSA. There are many facets of COMSEC, however, which do not require such rigid observance of special security rules. A number of cryptosystems have been removed from the category of those requiring cryptographic clearances before disclosure is authorized.

In any case, I do not indorse the proposal that a panel of communicators be established to review the security of COMINT and COMSEC operations. Both USCIB and USCSB are qualified and competent to take such actions on these matters as may be necessary.

NSA TS CONTL NO 551561A
COPY NUMBER _____
PAGE 3 OF 4 PAGES

TS# 179251-A
Page 3 of 4 pages
Copy 2 of 7 copies

~~TOP SECRET~~

TOP SECRET

TOP SECRET

7. Special Recommendation: That the President set up a special commission composed of technically qualified civil and military communications and electronics representatives, to survey and produce recommendations as to ways and means to insure the more effective utilization of all communications in case of war or national emergency.

Comment: I am not certain just what value the establishment of another special commission would have and, therefore, I do not support this recommendation.

8. The following comments are made on the narrative portion of the Report:

a. On pages 20 and 18 similar sets of figures are given on possible cryptographic compromises. I consider the narrative portion on page 20 to reflect more correctly the information which was provided to the Task Force.

b. Communications security, in the manner used beginning on page 16 is too narrow a definition because it refers to cryptographic security only. Consequently, the discussion immediately following the concept used concerns but one part of communications security. The definition contained in NSC 168 would be more appropriate.

c. The footnote appearing on the second page 19 greatly oversimplifies the calculation of "chances" for a cryptoviolation to occur. Using 5 as a multiplier implies that equal weight is given to the five processes in handling a message. I cannot agree with this assumption. Sending and relay station handling might compound a cryptographic error, but the basic violation would have occurred at the time of encryption. Similarly, the operations of receiving and decrypting have an insignificant effect on cryptosecurity. It is not apparent to me how the number of 8 serious violations was determined.

NSA TS CONTL NO 551561A
COPY NUMBER
PAGE 4 OF 4 PAGES

TOP SECRET

179251-A
Page 2 of 7 pages
Copy 7 of 7 copies